wallet. The user experience is similar to use wallet for external transfers. The implementation process of locking out is as follows:

[0080] (1) Initiate a Lock Out Request

[0081] User A operates in the wallet to initiate a transfer transaction of 10 BTC to an out-of-chain Bitcoin address, which is regarded as the user initiates a lock out request.

[0082] (2) Check, Lock in and Generate Transactions

[0083] The transaction triggers a lock out smart contract on the Fusion chain, the contract will first check the user A's asset status on the Fusion chain, when the transfer condition are met, lock in the status of 10 Bitcoins of user A in the Fusion chain account, and generate a transfer transaction with the target address and user's signature.

[0084] (3) Threshold Signature

[0085] The node on the Fusion chain receives the transaction instruction, to begin calculation and comparison based on the private key sharding of their respective stored, and the successful nodes will signature the result and broadcast it. Each node collects the signatures at same time, when the transaction signature reaches the requirement of t/m, ($t \leq m$) threshold, generally t/m is ⅔, the transaction is sent to the Bitcoin main chain by the node, and realize the transaction of transferring 10 BTC to the address specified by user A.

[0086] (4) Release Distributed Control Right Management

[0087] The nodes on the Fusion chain will check whether the transaction is confirmed on the Bitcoin main chain through the Bitcoin corresponding interface. When the consensus has reached the result of the transaction confirmation, the user A's 10 BTC will released from the distributed control right management.

[0088] (5) Release and Destroy Digital Assets

[0089] The smart contract synchronously updates the status of user's account on Fusion, and completes the release and destroy of the mapping by deducting the 10 locked in BTC mapping. At the same time, the lock out record is packaged and recorded into a block on the Fusion.

[0090] So far, the user's lock out request is completed.

[0091] Finally, when distributed control right transfer is completed, and then the state update of main chain account balance can reflect the completion of locking in (lock in) or locking out (lock out). The process of the accounting, the main chain actually issues or recovers the tokens used for accounting of the same amount of digital assets to the user account, thus completing the mapping of digital assets to the main chain or release mapping from it.

[0092] Using the mapping system and corresponding method to realize different digital assets on public blockchain based on distribute technology in the present invention, the mapping methods that supports different digital assets enables different currencies to be mapped to a mapping chain in a more innovative way, and no need to make any changes to any public chain, thus these tokens can realize multi-currency smart contact on the same chain, greatly improve the interoperability of the Internet of Value, and become the infrastructure of crypto finance. At the same time, the process of mapping is to securely control the private keys of tokens on various blockchains in a distributed manner, so as to establish a distributed blockchain that manages the control right of tokens. It is like the "highway" on the Internet of Value, which can easily realize value transfer between various tokens and multi-currency smart contracts for crypto finance services.

[0093] In this specification, the present invention has been described with the reference to its specific embodiments. However, it is obvious still may be made without departing from the spirit and scope of the present invention, various modifications and transformation. Accordingly, the specification and drawings should be considered as illustrative rather than restrictive.

I claim:

1. A mapping system to realize digital assets on the mapping chain based on distributed technology, characterized in that, the said system comprises a mapping chain and at least two public chains, the mapping chain generates a private key sharding based on distributed technology and completes the decentralized custodial of each private key sharding, and by locking in and locking out the digital assets in at least the two public chains, to completes cross-chain communication between at least the two public chains.

2. A method to realize locking in and controlling of digital assets based on the said system of claim **1**, characterized in that, the method comprises:

(A**1**) sending a request for locking in the digital assets in a public chain, and triggering a smart contract on the mapping chain for locking in the digital assets;

(A**2**) the mapping chain generates a private key sharding based on distributed technology, and completes the decentralized custodial of each private key sharding;

(A**3**) the public chain transfers control right of the digital assets to the mapping chain, in order to realize the distributed management of the digital assets;

(A**4**) confirming the successfully transferring of control right of the digital assets, and then the smart contract updates the account status of the mapping chain, in order to complete locking in and mapping of the digital assets.

3. The method to realize locking in and controlling of digital assets according to claim **2**, characterized in that, in the step (A**2**), the mapping chain generates the private key sharding based on the distributed key generation protocol DKG, and to decentralized custodial of each private key sharding.

4. The method to realize locking in and controlling of digital assets according to claim **3**, characterized in that, the decentralized custodial of each private key sharding is specifically:

saving each private key sharding in each node of the mapping chain.

5. The method to realize locking in and controlling of digital assets according to claim **4**, characterized in that, the step (A**3**) comprises:

(A**31**) the mapping chain generates a locked address of the public chain based on each private key sharding;

(A**32**) transferring the digital assets to the locked address, and initiate a transaction broadcast to the mapping chain of transferring the digital assets;

(A**33**) through the query interface, each node of the mapping chain confirms that the transaction of the digital assets is confirmed on the public chain, and then transfers the control right of the digital assets for which transaction has been completed.

6. A method to realize locking out and controlling of digital assets based on the said system of claim **1**, characterized in that, the method comprises: